STATE OF LOUISIANA
OFFICE OF FINANCIAL INSTITUTIONS
BATON ROUGE, LOUISIANA

Effective November 20, 2006;
Revised August 19, 2010

POLICY NO. OFI-EC-06-01

PROTECTION AND USE OF COMPUTER ASSETS AND INFORMATION

I. PURPOSE: To provide guidelines for physical and logical security of laptop computers, software installed on these computers, data contained on hard drives or in workpapers, peripheral equipment, other external media devices, or personal digital assistants (PDAs)/mobile devices

II. SCOPE: This policy applies to all employees using Louisiana Office of Financial Institution (OFI) PDAs/mobile devices, computers (primarily laptop computers), as well as all employees using external media devices to store non-public information obtained from entities regulated by OFI or confidential information related to regulation and/or examination of such entities. This also includes NCUA-assigned computers and associated computer equipment.

III. GENERAL:

Since the physical attributes, such as the size and weight of the machine, continue to decline, laptop computers are more easily carried from place to place. As technology has advanced, laptop computers have become more powerful, and their use has become more prevalent because of the flexibility they allow in today's working environment. However, because of this ease of transportation and increasing storage capacities, physical and logical security needed for laptops is essential, especially as it relates to potential loss of the laptop, including loss of or unauthorized access to data stored on the machine. Because of this, employees should always be aware of their surroundings when using laptop computers.

Security of laptop computers is not just limited to the hardware and software but also includes data stored on the hard drives and other external media devices, such as USB drives, or CDs/DVDs, that employees may keep with the computers. This is especially important if these devices contain non-public or confidential information from regulated entities, such as examination data, that can identify a specific financial institution or employee of the institution or customer data that personally identifies an individual.

All laptop computers, PDAs/mobile devices, external media devices to store computer information acquired for or on behalf of the OFI as well as the information shall be deemed to be property of the OFI. [NOTE: This includes NCUA-assigned computers and computer equipment.] **Each employee issued with a PDA/mobile device or laptop is responsible for the security of that equipment as well as any of its peripherals, including external media devices, regardless of whether the equipment is used in a financial institution, OFI's district or main offices, at the employee's**

residence, or in any other location such as a hotel, conference room, car, or airport. These responsibilities include protection from physical damage, theft, introduction of malicious codes or other malware, and inappropriate access to the computer or accompanying data and the protection against all forms of unauthorized access, use, disclosure, modification, or destruction to the information.

While a computer, computer equipment, external media devices, or information assets are in a vehicle, these item(s) should be placed in the trunk of a car or in a concealed/secure area of a truck until arriving at the final destination—never leave in an unlocked vehicle, even if the vehicle is in your driveway or garage, and never leave for an extended period or overnight, even if the vehicle is locked. Extra precautions should be given to when you leave a computer or its equipment in a vehicle, especially when you know that confidential information is on the computer or you know that you will be parked in an area which is prone to crime or has recently experienced a heightened amount of crime. When in doubt, leave the computer in the institution's vault (in accordance with the other rules delineated in this policy), locked up at the office, or ask a co-worker, who is not detouring on the way back to the office or home, to take it back to the office or home for you.

No OFI computer, peripheral equipment, or electronic medium will be made available to unauthorized person(s) for his/her/their use. In addition, no unauthorized peripheral equipment will be installed or connected to the OFI laptop computers, and no unauthorized personal computer will be connected to OFI peripheral equipment. [NOTE: This paragraph's limits on peripheral equipment exclude USB drives and printers utilized for work-related tasks. However, be sure to scan unfamiliar USB drives before used in OFI computers.]

IV. SPECIFIC:

Laptop Computers

Administrative Rights / User IDs

OFI's Information Technology (IT) Section makes sure that the laptop computers are configured to include common and specialized software used by OFI personnel and the various printers used before the laptops are assigned to the district offices (DOs) or employees at the Baton Rouge Main Office (BRMO). Because there are some instances where administrative rights are needed by field personnel, such as updates to software, the IT Section has found it necessary to provide each district's PC Coordinator with access to the administrative rights. Laptops do not require administrative rights to function properly. Microsoft Windows Operating System allows you to set up selected software with administrative rights if the programs require these rights to function normally. Therefore, PC Coordinators should only share this information with a designated backup and should only log on with these rights when needed.

PC Coordinators and their designated backup, who have access to the administrative rights, should not change the user ID and password set up by the IT Section. The IT Section will need administrative access if there are any issues that need to be addressed if the computer is sent back to the Main Office.

From this point forward, when a laptop is designated for an assignment to a DO, the PC Coordinator will establish a second user account with administrative rights for use only by themselves or their backups. The laptops are configured with a limited user account and default password. PC Coordinators should login with administrative rights, open the limited user account, and require the assigned employee to change the default password to a unique one. However, they should not change the USER ID because it will affect the access on the computer for the user.

Password Characteristics and Security

All computer passwords must (1) be at least eight characters long, (2) not spell a word, (3) use both the alphabet and numbers, and (4) include the following: one lowercase alphabetic character, one uppercase alphabetic character, one numeric character, and one special character (!@#$%^&*). Some reference materials recommend using a phrase to form a password, such as "Life is like a box of chocolates. Forrest Gump" to form the password, Li!bc4sg.

Even though Microsoft Windows Operating System or GroupWise does not have a setting for passwords to expire, each employee should reset his/her password every 30 days at a minimum in accordance with OFI's Authentication Policy, OFI-IT-03-03.

Do not write the password to the laptop computers on any paper material that does not remain under your focused control, do not attach the password to the laptop computer, do not store the password on a file in the laptop computer, or disclose the password to anyone. Do not write OFI's dial-in telephone number(s) and remote access password, OFI's GroupWise Web Access URL and your username and password, or OFI's Intranet Address on any paper material that is not under your focused control or disclose the telephone number(s) or passwords to any unauthorized person(s). In this paragraph, 'focused control' does not include writing passwords on paper that might be easily lost or identified. If written, passwords should be kept in a secure place like your wallet with special codes so that if lost, its function will not be easily identified.

It is a best practice not to use unfamiliar computers, such as ones in a hotel lobby, to access your GroupWise email account or OFI's Intranet website. If it is necessary to use an unfamiliar computer to access these sites, you should delete these sites from the Internet history and **NEVER** allow the operating system to "remember" your password, even when using your own or an OFI computer. However, if you used an unfamiliar computer that has a program installed on it that can record keystrokes, it won't matter that you have erased the history or did not save your username and password on the computer. The keystroke recording program will recall this highly confidential information allowing someone to access your emails or bank account or whatever keystrokes were recorded. If you use an unfamiliar computer to access password protected areas, a compensating control would be to change your password afterward as soon as possible to limit any potential unlawful use. It is also a good idea to save frequently used websites to your "Favorites" and purge your Internet history frequently so not to slow down your computer.

Hardware Configuration

Employees should not change the hardware and software configuration set by the IT Section including disabling firewalls.

Software Installation/Updates/Repairs

As noted above, most of the software commonly used by employees is installed by the IT Section before the laptops are assigned to specific DOs or employees. **Unauthorized installation of any software, including but not limited to, software applications, games, internet access, and messaging/mail programs is strictly prohibited.** Occasionally, the IT Section will send out software updates on external media devices for PC Coordinators to install, including patches issued to correct discovered vulnerabilities in the software. PC Coordinators must ensure that these updates are installed timely, and it is imperative that the PC Coordinator or designated backup install these updates on all laptops as soon as reasonably possible from the date of receipt.

All computers are configured to use a daily auto-update feature for the operating system, and the IT Section has configured the laptops with this same feature for the anti virus software. The auto-update feature, however, will only work when the laptop is connected to the Internet.

Employees are responsible for ensuring that these updates, especially for the antivirus software, are performed at least once every two weeks. However, employees can use this feature more frequently, as feasible, and should use the high-speed Internet connections now available at all of the DOs, if possible. Do not disable or stop the antivirus program that is automatically started when the laptop computers are turned on, and never stop the antivirus or patch management programs from updating your machine with the virus definition files or with the system security updates and patches.

Always run a virus scan on any new or unfamiliar external media devices before you place them in the laptop, especially when these items are received from others, including other federal examiners. Also, periodically check these items for viruses on a regular basis.

If an employee knows of a software program that has some business purpose that is useful in the performance of their job duties, they should ask their PC Coordinator to check with the IT Section (see Attachment A) on whether this software can be installed on their laptop. The IT Section's permission will constitute authorization to install the software. Otherwise, no unauthorized software will be installed on any OFI/NCUA computer.

Employees should not copy office software and should not use office software for other than office business. Employees should never disclose to unauthorized person(s) information on this office's software or equipment configurations.

In addition, all repairs to laptop computers and peripheral equipment will be performed by an authorized, contracted service provider as coordinated by the IT Section.

Laptop Use

Laptops are primarily assigned to the various OFI DOs and then assigned to district employees for performance of their assigned job duties. The District Office Manager (DOM) or his/her designee, such as the Assistant District Office Manager (ADOM) or PC Coordinator, should maintain a listing of laptops that shows a description of the laptop, the OFI Tag number and serial number, and name of the employee who has been assigned that particular computer. To avoid confusion among employees, laptops, computer accessories, and carrying bags should be easily identifiable. Do not leave any external media devices or any security token(s) in the laptop computer carrying case(s). These items must be kept in a separate location to prevent loss of information in the event the laptop computer is stolen and from unauthorized access when the laptop computer is locked in the institution's vault.

Employees are responsible for the care and maintenance of assigned laptops and should report any problems or issues related to the computer's operation to the PC Coordinator. PC Coordinators and their backups (when necessary) are mainly responsible for ensuring that updates distributed through the IT Section are installed properly and timely on the laptops assigned to their office. They should also try to address and/or correct any problems related to the operation of the computers that employees report to them with consultation of the IT Section if necessary.

Employees should only access system areas, functions, or files that they are formally authorized to use and should only access OFI systems and networks with assigned username and password.

Workplace Environment and Physical Security

Because the laptops are OFI property, they should always be available for use during working hours. However, OFI employees should always be aware of the environment in which they are working to ensure proper security for the laptops. Do not leave laptop computer(s), peripheral equipment, or external media devices unattended for any length of time. Employees should make sure laptops are properly secured or stored to deter possible loss, primarily from theft, when not in use or the employees are away from their work area for an extended period of time. If necessary, this may consist of a locking file cabinet or other secured area. Do not leave your laptop overnight at the financial institution unless the authentication token is removed and the laptop is locked in the institution's vault, in a secure, locked room (not accessible to any institution employees, including janitorial service), or locked file cabinet. Otherwise, take it with you. Even if the laptops are left locked in the vault or a secure room, take all external media devices and the authentication token with you.

The employee should use a password protected screensaver as described below under "Password Protected Screensavers" if they are working in an area that is accessible only to other OFI employees or employees of the entity being examined. However, if the employee must leave the computer unattended, they should exercise more care in securing the computer, which should include removing the authentication token from the computer and storing the computer in a locking file cabinet or attaching the computer to a secure, stable object via a cable lock system. In an area easily accessible to the public, the employee should exercise extreme care in securing the computer even when the employee is only away from his/her work station for a short period of time.

When working at home with a computer, place the computer in a safe, inconspicuous area. It is strongly encouraged to use OFI's computer when working at home and not your own personal computer. In the event that you perform work at home on your own personal computer involving non-public or confidential information or exam data, the work should be done directly from the external media device and saved back to the external media ~~storage~~ device. No non-public or confidential information should be transported and saved to one's personal home computer.

Unless the DO's external doors remain locked, when working in the office with a computer, tether the laptop to a secure, stable object via a cable lock system during the day and lock the laptops up at night. DO external doors should remain locked unless an authorized person has a focused control of the area. In this paragraph, 'focused control' does not include someone in the rear of the office with the front door unlocked. If the doors frequently remain unlocked without focused control of the area and you are unable or unwilling to tether the laptop to a secure, stable object, the laptop should be locked away whenever you are away from it.

Never leave external media devices or authentication tokens with the computer, in the computer's carrying case, or unattended on a desk.

Hard Drive Encryption

OFI is still utilizing USB authentication tokens for some OFI laptop computers. When a USB authentication token is used, each token will be configured to a specific computer and will only work with that computer. The encryption process does not encrypt certain files, such as program files and Windows files; therefore, non-public and confidential information should NEVER be saved to any files that are not encrypted by the authentication process. Without the token, the laptop is not usable; therefore, theoretically, the hard drive is not readable even if removed from the computer. Once configured to a computer, the user plugs the token in when booting up or anytime that a password is required. By entering the password, the hard drive will be decrypted. Then, the authentication token should be removed and retained in a safe place separate from the computer. Upon shutdown, hibernate, or standby, the hard drive will become encrypted. The authentication token does not have to be inserted for the encryption of the hard drive. The token should NEVER be stored with the computer. If the token is lost, the IT Section should be contacted immediately for alternate methods of accessing the computer and replacing the token.

OFI's IT Section is in the process of replacing the USB authentication tokens with Full Disk Encryption Hard Drives. Unlike the USB authentication tokens, the Full Disk Encryption Hard Drives encrypt everything including program files, Windows files, and the programs bootable operating system partitions. By the end of calendar year 2010, only 12 laptops will still have the USB authentication tokens. If budget permits, the remaining 12 laptops with the USB authentication tokens will be replaced with Full Disk Encryption Hard Drives by September 2011.

Travel with Laptops

On occasion, OFI employees may be required or choose to bring their laptops to various regulatory schools. When traveling by air, employees must always treat the laptop as a carry-on item and never as checked baggage. Because most are similar in appearance, carrying bags should be easily identifiable. Watch your laptop at all times as it enters and exits the airport x-ray machine. Thieves have been known to work in pairs to create a diversion at the x-ray area of airports, allowing one thief to walk off with the laptop as it exits the x-ray machine, while the other holds up the x-ray machine line by having to re-enter the scanning device numerous times.

When traveling by automobile, OFI personnel should ensure that laptops are appropriately secured. For example, if an employee traveling alone should have to leave the car unattended, they should lock the vehicle and ensure the laptop is not in plain sight. If necessary, employees should take the laptop with them rather than leave it in a vehicle for an extended period of time because extreme temperatures may cause damage to computers or the external media devices.

When staying in a hotel, place the computer in a safe, inconspicuous area or with the hotel's concierge but separate from the external media device and authentication token.

Password Protected Screensavers

It is recommend that all computers have a password-protected screen saver set at a maximum of 15 minutes of inactivity (shorter if more appropriate in the current working environment) to lock the computer when away from it. This may deter possible compromise of information on the laptop, such as viewing or copying of data by an unauthorized person when the employee is away from the computer for short periods of time. Employees should only use a password protected screensaver when they are away for short periods of time. More care should be taken if the employee must leave the computer unattended for longer periods.

Desktop Computers

Desktop Use

Most of the items listed in this document for laptop computers will also apply to desktop use; however, if a desktop computer is connected to the BRMO network, non-public or confidential information should not be stored on the hard drive of the desktop computer. All non-public and confidential data should be stored on the network drive (F: drive). The DOs may use the network drive as a method of securely saving non-public or confidential information, but they may also use the local (C: drive) as they would with a laptop closely following all of the security precautions.

Information Security

Periodic Review of Hard Drive

At least quarterly or more frequently, if needed, employees should review the contents of their laptop's hard drive to remove any unnecessary information. When reviewing hard drive contents, employees should only maintain current work in progress. **Employees should remove all "not in-process" data but may backup this information to CDs/DVDs that are stored in a secure location.** Examinations deleted through GENESYS or AIRES, the software used for bank/thrift and credit union examinations, will automatically delete the folders and documents that it originally created. GENESYS or AIRES examinations should be considered "not-in-process" once a final report has been issued by this office.

Electronic data files received from the financial institution which contains confidential personal customer information should be destroyed after transferring the information to a secure network drive or into the GENESYS, ALERT, or AIRES (for credit unions) program. All other data files should be safely stored with the examination workpapers.

Employees should also delete documents that they create through programs such as Word and Excel if those documents contain non-public or confidential information. Employees may maintain data/documents on their hard drive for future reference (commonly called "go-bys"); however, this data should not contain any references that would disclose confidential information related to a regulated entity, examination data that can identify a specific financial institution or employee of the institution, or customer data that personally identifies an individual. Examples of such information would include: an FDIC Certificate Number, a credit union charter number, an OFI License Number, officer's name, or a customer's name and loan or social security number.

Employees should also review the hard drive's contents and delete unnecessary data if their computer is being reassigned to another individual as well as when it is turned in for replacement by newer equipment. Employees should not delete files if they are unsure if deletion will affect the normal operation of a specific software program.

All OFI computers should have similar file setups with uniform standards in which confidential files are saved to the hard drive. This will make it easier for employees and managers to periodically review the hard drive to ensure that non-public and confidential information is removed.

DOMs have the right to review the hard drive contents for OFI laptops assigned to their district employees. DOMs, or their designee, should review the hard drive contents for all laptops on an ongoing basis, at least annually, to ensure that all employees are removing unnecessary data from their laptop hard drives. The DOM should maintain records of the hard drive checks for an annual review by the BRMO.

Suggestions for methods to review the hard drive follow:

(1) In Windows Explorer, click on the folder(s) that you wish to review, select the 'Search' button, click on the 'All files and folders' button, and the 'When was it modified?'

button. Then, you will select the dates that you wish to review, and hit 'Search.' All files and folders that were modified between the dates selected will be listed, and the DOM or his designee may review files that may have confidential information in them.

(2) In Windows Explorer, click on the folder(s) that you wish to review, select the 'Search' button, click on the 'All files and folders' button, and specifically list words that may be suspicious in the "A word or phrase in the file:" section, such as "customer number," "CIF," "loan number," "account number," "social security number," etc. Using this method, the program will only look for the exact word that you type in, so it may not find 'social security number' because 'SSN' is used. With this method, you may also review for specific dates that the file was modified, created, or accessed.

USB Drives (one form of external media device)

USB drives have become an essential item in the transfer of data between computers, especially in the Banking Section of OFI. All USB drives currently used allow for password protection and/or encryption; therefore, a third party should not be able to access stored information simply by plugging the USB drive into the USB connection of another computer. Regardless of the protection provided, employees should limit the information they maintain on these USB drives, exercise care in ensuring that the USB drive is kept in a secure location when not in use, and immediately erase information at the completion of the transfer of examination information or other confidential data from one computer to another. Employees should review the contents of the USB drive on a more frequent basis than the hard drive and delete any unnecessary information.

Data from Outside Sources

When receiving information from outside sources, such as through an e-mail attachment or CD/DVD, employees should always run a virus scan to check for viruses. Once the scan is finished and provided it detects no virus threat, the employee can then open the file as needed. If information requested may contain non-public or confidential information, employees should never request that it be e-mailed unless the information is encrypted at a minimum of 128-bit. If the document is also password protected, the employee should ask the sender to provide the password through a telephone call and never put it in the e-mail message sent with the requested information.

Employees should not use peer-to-peer technology for non business purposes including transferring of music, movies, software, and other intellectual property.

Storage and/or Destruction of Data

Examiners should ensure that non-public and confidential information resident on hard drives or external media devices and paper is not seen by unauthorized parties. Employees should delete information on hard drives once that information is no longer needed. Any electronic media devices used to transfer examination information from one laptop computer to another should be immediately erased at the completion of the transfer. Employees should properly store information on CDs/DVDs and paper in a secure location. When the information is no longer needed, employees should destroy/shred the CD/DVD, return the CD/DVD to the sender for destruction (if applicable), and shred any paper documents containing non-public or confidential information.

All OFI information assets printed at the office or at the institution's site must be shredded before discarding. If the institution's site does not have a paper shredder, all OFI information assets printed at the institution's site or as part of an examination must be brought back to the office and properly shredded before discarding.

Confidential Information

Transporting Confidential Information

When transporting work papers and other confidential information, the DOM or his/her designee should maintain a list of specific items containing institution customer information and any other confidential information separate from the work papers in the event of theft or loss. If work papers or other confidential information is mailed, the DOM or his/her designee should track the transport of these items to ensure timely receipt of all shipments.

Limited Use of Confidential Customer Information

Copying documents containing confidential institution customer information, such as customer loan applications and tax returns for credit analysis purposes, should be discouraged. For example, necessary number from customer loan applications and tax returns for credit analysis purposes should be transcribed to loan tabs. In the event that there is no alternative, the work papers should be marked confidential and properly disposed of as soon as work paper retention periods expire.

Other Laptop Issues

Wireless Internet Connectivity

[NOTE: As long as wireless connectivity is utilized through a VPN or other NCUA secured connection, the NCUA computers are excluded from this prohibition on wireless usage.]

Although the laptops may have wireless capabilities, this feature is disabled in the initial setup of the laptops **except for depository field examiners**. While wireless technology and its usage have become more prevalent, the lack of security in a wireless network environment remains a significant concern. Because of these concerns, the IT Section has researched, tested, and authorizes only OFI issued MiFi 2200 Mobile Hotspot devices issued to each district office for wireless use by the depository field examiners. Any other use of wireless capabilities is strictly prohibited. Therefore, employees shall not alter the wireless capabilities of the laptops.

Windows Firewall

All depository field examiners laptops have a Firewall application installed. Laptops are configured with the firewall turned on, and employees **should never disable** this function.

Pop-up Blocker

Internet Explorer (IE) has Pop-up Blocker built into it. Employees should ensure that this feature is enabled and set to at least Medium, which blocks most automatic pop-ups. To check the status of Pop-up Blocker, open IE and click on Tools on the menu bar. When you see Pop-up Blocker and two additional commands, "Turn Off Pop-up Blocker" and "Pop-up Blocker Settings…", this feature is enabled. The settings on this feature will let users allow pop-ups on an individual website basis as some sites may require this to function properly.

Spyware and Adware

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. **Adware** is software that displays advertisements on your computer and can inexplicably pop up on your screen even when you're not browsing the Internet.

Spyware and Adware can cause a number of problems with the operation of your computer, including taking a longer time to complete certain tasks, changing the home page on your web browser without your consent, and causing your computer to crash more often. The easiest ways to avoid potential issues with this is to adhere to the OFI E-mail, Internet, and Telephone Use Policy (EC-03-01), stay off unfamiliar web sites, and always click the "X" in the upper right hand corner of the window if an ad or pop-up appears on your screen.

Security Incident Response Programs

Actual or Suspected Incidents of Abuse

All actual or suspected instances of information asset or equipment theft and abuse, as well as potential threats (e.g. hackers, computer viruses, fire) or obvious control weaknesses affecting security, must be reported immediately to the DOM and the IT Section (see Attachment A).

Damage to Computer or Associated Computer Equipment

If an OFI computer or associated computer equipment is damaged, the employee assigned responsibility for the computer/equipment should do the following as soon as possible but no later than the next business day:

1. Notify your DOM or direct supervisor as soon as possible but no later than the next business day.
2. Provide a written damage report describing details surrounding the damage (see Attachment B) to the DOM or direct supervisor. The supervisor will provide a copy of the damage report to the appropriate DCE. If the damage was to a NCUA-assigned computer, the employee will have to complete a Report of Unserviceable, Lost, or Damaged Property report that may be obtained from the NCUA's OCIO help desk.

Computer, PDA/Mobile Device, Documents, or Media Theft

If an OFI computer, PDA/mobile device, documents, or media is stolen, the employee assigned responsibility for the computer should do the following (items 1 and 2 within 1 hour of discovering the incident):

1. Notify the appropriate law enforcement agency and request to file a police report.
2. Immediately notify your DOM or direct supervisor of theft/loss and include what equipment was stolen/lost, if it is possible that password(s) could be compromised, and whether authentication token or smart cart (for NCUA computers) is still in employee's possession. The direct supervisor will notify the Deputy Commissioner (DC) or Commissioner within the 1st hour of discovery. [NOTE: Notification from supervisor to DC and Commissioner may be done all at once through Blackberry or Groupwise email, and this email should also include the CE and DCE.]
3. Make arrangements with OFI's IT Section (see Attachment A) for the return of your authentication token.
4. File police report and obtain a copy as soon as it becomes available.
5. Provide written incident report describing details surrounding the theft (see Attachment C). Also, include details of information stored on the laptop. If the theft/loss was to a NCUA-assigned computer, the employee will also have to complete a Report of Unserviceable, Lost, or Damaged Property Report that may be obtained from the NCUA's OCIO help desk.

Theft or Loss of Institution Customer Information

Once OFI becomes aware that a computer containing institution customer information or confidential examination data is stolen or lost, the following events will occur:

1. The Governor's Office will be notified by the Commissioner or DC.
2. The institution whose customer information or examination data has been compromised will be notified of the theft or loss.
3. The primary federal regulator will be notified.
4. Arrangements will be made with the institution and federal regulator for institution customer notification.
5. OFI legal counsel and senior management will prepare any needed press releases and procedures for handling calls from the press and institution customers.

It will be extremely important that all external communications be handled professionally. Such a loss has the potential to greatly harm the reputation and credibility of the OFI. Liability to OFI and the individual examiner will potentially exist.

Compliance with Policy

All employees of OFI shall comply with this policy and associated information security directives. Information systems must not be installed or used in such a manner as to provide the opportunity to create unauthorized links to other systems, bypass authentication mechanisms, circumvent data access control procedures, or otherwise jeopardize the security of any or all components within the OFI network.
Employees should understand that OFI reserves the right to audit, monitor, and/or log all network activity including computer dial-up access and Internet access, with or without notice, to reveal security and policy violations; therefore, employees should have no reasonable expectation of privacy in the use of these resources. Employees should not attempt to monitor or tamper with another user's electronic communication or read, copy, change, or delete another user's files or software without the explicit agreement of the owner or appropriate program management direction.

All violations of OFI's security policies and/or procedures are subject to disciplinary action. The specific disciplinary action to be rendered will be dependent upon the nature of the violation, the impact of the violation on OFI's information assets and related facilities, etc.

Violation of Policy

Disciplinary action, up to and including termination of employment, may be exercised in the event that these policies have not been followed. If an employee's laptop, PDA/mobile device, or authentication token is stolen, lost, or damaged and the employee is deemed negligent, the employee will be held responsible for reimbursing OFI for the replacement costs.

John Ducrest

____________________________	08/19/10
John Ducrest Commissioner of Financial Institutions	Date

JDF/TLR/KLM/DR

| = Denotes changes made when policy was revised.

Attachment A

(As of August 19, 2010)

(1) Person responsible to authorize software to be added to computer and to notify of theft:

IT Section
Baton Rouge Main Office

Danny Ragan
225/925-4308
dragan@ofi.louisiana.gov

Mike Cross
225/925-3776
mcross@ofi.louisiana.gov

Christopher Dupre
225/925-3658
cdupre@ofi.louisiana.gov

Wangson Sylvien
225/925-4535
wsylvien@ofi.louisiana.gov

(2) Person responsible for computer inventory:

Kathleen Parrish
HR Analyst
Baton Rouge Main Office
225/922-0630
kparrish@ofi.louisiana.gov

If the persons listed above are not available in an instance in which the policy requires contacting one of them, you may contact the IT specialist in the depository review section (Tim Robichaux—225-922-0878), or a depository Deputy Chief Examiner (Kerry Morris—225/925-4201 or John Fields—225/922-0633).

ATTACHMENT B

DAMAGE REPORT

8/10

The Louisiana Office of Financial Institutions' Damage Report Form must be completed whenever any damage has occurred to an OFI-assigned computer, computer related equipment, or PDA/mobile device. For this report, 'damage' will not include a malfunction of the computer, related equipment, or PDA/mobile device. Malfunctions should be reported directly to the IT Section.

EMPLOYEE NAME: ____

DATE/TIME OF DISCOVERY: ____________________/__________________

LOCATION OF INCIDENT: ____

LIST OF COMPUTER EQUIPMENT DAMAGED (include serial numbers):
1.

As soon as possible or within 1 business day of discovering damage to a computer, related equipment, or PDA/mobile device, the employee assigned responsibility for the equipment should do the following:

1. Date/Time (__________/__________) I notified DOM or direct supervisor. Note name of DOM or direct supervisor notified: ____________________________.

2. Provide details of how damage occurred and name(s) of employee(s) involved.

   ____

   ____

   ____

   ____

   ____

   ____

   ____

3. Date/Time (__________/__________) [ ] I or [ ] supervisor provided a copy of this report to DCE. Copy to DCE ______________ was provided by _________________.

ATTACHMENT C

INCIDENT REPORT

8/10

The Louisiana Office of Financial Institutions' Incident Report Form must be completed whenever any OFI- or NCUA-assigned computer, computer related equipment, information assets, or PDA/mobile device have been lost or stolen.

EMPLOYEE NAME: ____

TIME OF DISCOVERY: ______________________________________

LOCATION OF INCIDENT: ____

LIST OF EQUIPMENT DAMAGED (include serial numbers):

1.

Is the authentication token/smart card in your possession? [ ]Yes [ ]No
Is it possible that any password(s) could be compromised? [ ]Yes [ ]No

LIST OF INFORMATION ASSETS MISSING:

1.

Within 1 hour of discovering a theft or loss of computer, equipment, or information assets, or PDA/mobile device, the employee assigned responsibility for the equipment or information assets should perform items 1, 2, and 3. The other items should be completed as soon as possible or by the next business day.

1. Date/Time (____________/____________) I notified the appropriate law enforcement agency and requested to file a police report. Note name of law enforcement agency notified: ____.

2. Date/Time (____________/____________) I notified DOM or direct supervisor. Note name of DOM or direct supervisor notified: ______________________________.

3. Date/Time (____________/____________) [ ] I or [ ] supervisor notified [ ]Commissioner or [ ] Deputy Commissioner. Name of person notifying Commissioner/DC is ______________________________. If notification was done by email, attach a copy of email.

4. Date/Time (______/______) [ ] I or [ ] supervisor (____________) notified IT Manager. The arrangement made with the IT Section was that I would do the following:

   ____

   ____

   ____

   These instructions were completed on: ______________________________.

5. Date/Time (____________/____________) I filed the police report with __(Name of Officer)______________. A copy of the police report [ ] is [ ] is not attached. If a copy of the police report is not attached, note the approximate date that a copy will be available: ____________________________. [NOTE: The employee will obtain a copy of the policy report and attach it to this report.]

6. Attach separate written report describing details surrounding the incident.

If information assets containing confidential information were included on the stolen or lost equipment, the BRMO will complete the following additional questions.

7. Date/Time (____________/____________) Commissioner notified Governor's Office.

8. Date/Time (____________/____________) __________________________ notified the institution. ______(Name of person)____________ was notified with _____(Name of Institution)____________________________.

9. Date/Time (____________/____________) __________________________ notified the primary federal regulator. In this case, the primary federal regulator was __________. ___(Name of person)___________________ was notified with that office.

10. Date/Time (____________/____________) Commissioner notified legal counsel (________________________________) and senior management (__________________________) to begin work on a press release and procedures for handling calls from the press and institution customers. The press release and procedures to be utilized are attached.

An attachment describes the arrangements made with the institution and the appropriate federal regulator to notify customers. Date notification was completed: ___________________________

A copy of this completed document should be retained by the manager, the appropriate DCE, and placed in the employee's personnel file.

SUBJECT: **Computer Hardware Administrative Controls**

EMPLOYEE ACKNOWLEDGEMENT

LOUISIANA OFFICE OF FINANCIAL INSTITUTIONS (OFI) EQUIPMENT FORM 8/10

EMPLOYEE NAME: ____

LAPTOP SERIAL / OFI TAG NUMBER: _____________________________________

The following statements pertain to the use, care, maintenance, and safekeeping of assigned computer hardware or PDA/mobile device.

- OFI issued Computer Hardware is to be used for business purposes only.
- OFI Computer Hardware and PDAs/mobile devices should be properly stored or secured when not being utilized.
- All information (files/directories/etc.) stored on OFI issued Computer Hardware and PDAs/mobile devices should be considered confidential, work product, and privileged. As such, all steps including passwording and/or encryption or other security methods should be utilized to ensure its safekeeping.
- Loss of the OFI issued Computer Hardware or PDA/mobile device must be immediately reported to the employee's direct supervisor and the IT Section at OFI's Main Office.
- All OFI issued Computer Hardware and PDAs/mobile devices are the property of the State of Louisiana. They shall be returned upon request or upon retirement/termination of employment with the OFI. Damaged or broken Computer Hardware or PDAs/mobile devices should be immediately returned to the OFI IT Section.

○ I acknowledge receipt of a (Make)_______________________ and (Model #)__________.

○ I agree to keep the authentication token separate and apart from the laptop/notebook when not in use.

○ I agree to surrender the authentication token immediately upon loss of the laptop/notebook.

○ I acknowledge receipt of a _______(Brand)_______________ _______MB USB DRIVE.

○ I acknowledge receipt of a Travel Case, power cords, and software.

○ I acknowledge receipt of a PDA/mobile device (Make)_____________________________ and (Serial #)____________________________________.

○ I agree to maintain compliance with the requirements contained in OFI's Protection and Use of Computer Assets and Information Policy effective September 20, 2006, updated October 24, 2007, and updated August 19, 2010.

Name Printed: _______________________________

Signed: ____________________________________ Date: ________________________